Amendments to the Claims

Please cancel claims 1-9, 51-96 and 128-140. Please amend claims 10, 20, 28, 37, 44, 97-102 and 106-127. Please add new claims 141-151. The currently pending claims are listed below.

1 - 9. (Cancelled)

10. (Currently Amended) A method for using verified information concerning a tangible object, comprising the steps of:

accessing descriptor data associated with the tangible object, said descriptor data including an identity public key for transforming data according to a first public/private key encryption algorithm, attribute data containing information concerning said tangible object, and a digital signature;

verifying that said digital signature matches said identity public key and said attribute data;

performing a pair of complementary data transformations on source test data to produce resultant test data, said pair of complementary data transformations being performed by:

(a) performing a first data transformation according to said first public/private key encryption algorithm using said identity public key, and

(b) accessing a digital protection system <u>physically</u> attached to said tangible object to perform a second data transformation according to said first public/private key encryption algorithm using an identity private key in said digital protection system, said identity private key corresponding to said identity public key according to said first public/private key encryption algorithm, said second data transformation being complementary to said first data transformation, <u>said digital protection system being a tangible device which receives input data, processes data, and produces output data independently of said tangible object</u>;

comparing said source test data with said resultant test data; and

using said attribute data in a manner dependent on the results of said step of verifying that said digital signature matches said identity public key and said attribute data, and said step of comparing said source test data with said resultant test data.

11. (Original) The method for using verified information concerning a tangible object of claim 10, wherein said digital signature represents an encryption of data derived from said identity public key and said attribute data according to a derivation algorithm, said encryption being according to a second public/private key encryption algorithm using a signature private key, and wherein said step of verifying that said digital signature matches said identity public key and said attribute data comprises:

decrypting said digital signature according to said second public/private key encryption algorithm using a signature public key;

deriving data from said identity public key and said attribute data using said derivation algorithm; and

comparing the decrypted digital signature to the data derived from said identity public key and said attribute data according to said derivation algorithm.

12. (Original) The method for using verified information concerning a tangible object of claim 11, wherein said derivation algorithm comprises a hash function.

13. (Original) The method for using verified information concerning a tangible object of claim 11, wherein said derivation algorithm is an identity function which produces as output an identical copy of the input.

14. (Original) The method for using verified information concerning a tangible object of claim 10, wherein said first data transformation is an encryption of said source test data and said second data transformation is a decryption of said source test data encrypted by said first data transformation, said first data transformation being performed before said second data transformation.

15. (Original) The method for using verified information concerning a tangible object of claim 10, wherein said second data transformation is an encryption of said source test data and said first data transformation is a decryption of said source test data encrypted by said second data transformation, said second data transformation being performed before said first data transformation.

16. (Original) The method for using verified information concerning a tangible object of claim 10, wherein said step of accessing descriptor data comprises obtaining said descriptor data from said digital protection system.

17. (Original) The method for using verified information concerning a tangible object of claim 10, wherein said source test data is randomly generated data.

18. (Original) The method for using verified information concerning a tangible object of claim 10, wherein said tangible object is a digital data processing device having at least one processor external to said digital protection system.

19. (Original) The method for using verified information concerning a tangible object of claim 10, wherein said digital protection system of said tangible object includes a coupling for mating with a local digital data processing device separate from said tangible object.

20. (Currently Amended) A program product for using verified information concerning a tangible object, said program product comprising a plurality of processor executable instructions recorded on signal-bearing media, wherein said instructions, when executed by a processor of a digital data processing device, cause the digital data processing device to perform the steps of:

accessing descriptor data associated with the tangible object, said descriptor data including an identity public key for transforming data according to a first public/private key encryption algorithm, attribute data containing information concerning said tangible object, and a digital signature;

verifying that said digital signature matches said identity public key and said attribute data;

performing a pair of complementary data transformations on source test data to produce resultant test data, said pair of complementary data transformations being performed by:

(a) performing a first data transformation according to said first public/private key encryption algorithm using said identity public key, and

(b) accessing a digital protection system physically attached to said tangible object to perform a second data transformation according to said first public/private key encryption algorithm using an identity private key in said digital protection system, said identity private key corresponding to said identity public key according to said first public/private key encryption algorithm, said second data transformation being complementary to said first data transformation, said digital protection system being a tangible device which receives input data, processes data, and produces output data independently of said tangible object;

comparing said source test data with said resultant test data; and

using said attribute data in a manner dependent on the results of said step of verifying that said digital signature matches said identity public key and said attribute data, and said step of comparing said source test data with said resultant test data.

21. (Original) The program product for using verified information concerning a tangible object of claim 20, wherein said digital signature represents an encryption of data derived from said identity public key and said attribute data according to a derivation algorithm, said encryption being according to a second public/private key encryption algorithm using a signature private key, and wherein said step of verifying that said digital signature matches said identity public key and said attribute data comprises:

decrypting said digital signature according to said second public/private key encryption algorithm using a signature public key;

deriving data from said identity public key and said attribute data using said derivation algorithm; and

comparing the decrypted digital signature to the data derived from said identity public key and said attribute data according to said derivation algorithm.

22. (Original) The program product for using verified information concerning a tangible object of claim 21, wherein said derivation algorithm comprises a hash function.

23. (Original) The program product for using verified information concerning a tangible object of claim 21, wherein said derivation algorithm is an identity function which produces as output an identical copy of the input.

24. (Original) The program product for using verified information concerning a tangible object of claim 20, wherein said first data transformation is an encryption of said source test data and said second data transformation is a decryption of said source test data encrypted by said first data transformation, said first data transformation being performed before said second data transformation.

25. (Original) The program product for using verified information concerning a tangible object of claim 20, wherein said second data transformation is an encryption of said source test data and said first data transformation is a decryption of said source test data encrypted by said second data transformation, said second data transformation being performed before said first data transformation.

26. (Original) The program product for using verified information concerning a tangible object of claim 20, wherein said step of accessing descriptor data comprises obtaining said descriptor data from said digital protection system.

27. (Original) The program product for using verified information concerning a tangible object of claim 20, wherein said source test data is randomly generated data.

28. (Currently Amended) A method for updating attribute data associated with a tangible object, comprising the steps of:

receiving a request to a service provider from a requestor to update said attribute data, the request including an identity public key for transforming data according to a first public/private key encryption algorithm, old attribute data, and an old digital signature of said old attribute data and said identity public key;

verifying that said old digital signature matches said identity public key and said old attribute data;

performing a pair of complementary data transformations of source test data to produce resultant test data, a first of said pair of complementary data transformations being performed by said service provider according to said first public/private key encryption algorithm using said identity public key, and a second of said pair of complementary data transformations being performed by requesting a digital protection system physically attached to said tangible object to perform said second data transformation according to said first public/private key encryption algorithm using an identity private key in said digital protection system, said identity private key corresponding to said identity public key according to said first public/private key encryption algorithm, said digital protection system being a tangible device which receives input data, processes data, and produces output data independently of said tangible object;

comparing said source test data with said resultant test data, said comparing step being performed by said service provider; and

depending on the results of said step of comparing said source test data with said resultant test data, generating an updated descriptor, said updated descriptor comprising said identity public key, updated attribute data, and ~~a~~ an updated digital signature of said identity public key and said updated attribute data.

29. (Original) The method for updating attribute data of claim 28, wherein said step of generating an updated descriptor comprises generating said digital signature by encrypting a derivation of said identity public key and said updated attribute data according to a second public/private key encryption algorithm using a signature private key.

30. (Currenlty Amended) The method for updating attribute data of claim 28, wherein said ~~request to update attribute data includes old attribute data and an old digital signature, said~~ old digital signature ~~representing~~ represents an encryption of data derived from said identity public key and said old attribute data, said encryption being according to a second public/private key encryption algorithm using a signature private key, said ~~method further~~ step of verifying that said old digital signature matches said identity public key and said old attribute data comprising:

decrypting said old digital signature according to said second public/private key encryption algorithm using a signature public key;

comparing the decrypted old digital signature to said data derived from said identity public key and said old attribute data to verify said attribute data;

wherein said step of generating an updated descriptor further depends on the results of said step of comparing the decrypted old digital signature to said data derived for said identity public key and said old attribute data.

31. (Original) The method for updating attribute data of claim 28, wherein said first of said pair of complementary data transformations is an encryption of said source test data and said second of said pair of complementary data transformations is a decryption of said source test data encrypted by said first transformation, said first transformation being performed before said second transformation.

32. (Original) The method for updating attribute data of claim 28, wherein said second of said pair of complementary data transformations is an encryption of said source test data and said first of said pair of complementary data transformations is a decryption of said source test data encrypted by said second transformation, said second transformation being performed before said first transformation.

33. (Original) The method for updating attribute data of claim 28, wherein said service provider is remote from said tangible object.

34. (Original) The method for updating attribute data of claim 33, wherein said tangible object is coupled to a local device, said local device communicating remotely with said service provider.

35. (Original) The method for updating attribute data of claim 28, further comprising the step of accessing a database in said service provider to verify that the requestor is entitled to the requested update.

36. (Original) The method for updating attribute data of claim 28, wherein said source test data is randomly generated data.

37. (Currently Amended) A method for using verified information concerning a tangible object, comprising the steps of:

accessing descriptor data associated with the tangible object, said descriptor data including an identity public key for transforming data according to a first public/private key encryption algorithm, attribute data containing information concerning said tangible object, and a digital signature, wherein said digital signature represents an encryption of data derived from said

identity public key and said attribute data according to a derivation algorithm, said encryption being according to a second public/private key encryption algorithm using a signature private key;

decrypting said digital signature according to said second public/private key encryption algorithm using a signature public key;

deriving data from said identity public key and said attribute data using said derivation algorithm;

comparing the decrypted digital signature to the data derived from said identity public key and said attribute data according to said derivation algorithm;

generating random source test data;

performing a pair of complementary data transformations of said source test data to produce resultant test data, including:

(a) performing a first data transformation of said pair of complementary data transformations according to said first public/private key encryption algorithm using said identity public key, and

(b) accessing a digital protection system physically attached to said tangible object to perform a second data transformation of said pair of complementary data transformations, said second data transformation being according to said first public/private key encryption algorithm using an identity private key in said digital protection system, said identity private key corresponding to said identity public key according to said first public/private key encryption algorithm, said digital protection system being a tangible device which receives input data, processes data, and produces output data independently of said tangible object;

comparing said random source test data with said resultant test data; and

using said attribute data in a manner dependent on the results of said step of comparing the decrypted digital signature to the data derived from said identity public key and said attribute data, and said step of comparing said random source test data with said resultant test data.

38. (Original) The method for using verified information concerning a tangible object of claim 37, wherein said first data transformation is an encryption of said source test data and said second data transformation is a decryption of said source test data encrypted by said first data transformation, said first data transformation being performed before said second data transformation..

39. (Original) The method for using verified information concerning a tangible object of claim 37, wherein said second data transformation is an encryption of said source test data and said first data transformation is a decryption of said source test data encrypted by said second data transformation, said second data transformation being performed before said first data transformation.

40. (Original) The method for using verified information concerning a tangible object of claim 37, wherein said step of accessing descriptor data comprises obtaining said descriptor data from said digital protection system.

41. (Original) The method for using verified information concerning a tangible object of claim 37, wherein said derivation algorithm comprises a hash function.

42. (Original) The method for using verified information concerning a tangible object of claim 41, wherein said hash function belongs to the set consisting of SHA-1 and MD5.

43. (Original) The method for using verified information concerning a tangible object of claim 37, wherein said digital protection system is implemented in digital logic contained on a single integrated circuit substrate.

44. (Currently Amended) An apparatus for verifying information concerning a tangible object, comprising:

a programmable processor;

a memory for storing instructions executable on said programmable processor;

a digital protection system interface coupled to said processor, said interface communicating with a digital protection system for said tangible object, said digital protection system being a tangible device physically attached to said tangible object which receives input data, processes data, and produces output data independently of said tangible object;

a protection system verification program executable on said programmable processor, wherein said protection system verification program

(a) obtains a data descriptor from a said digital protection system through said interface, said data descriptor comprising an identity public key for transforming data according to a first public/private key encryption algorithm, attribute data containing information concerning said tangible object, and a digital signature;

(b) verifies that said digital signature matches said identity public key and said attribute data;

(c) performs a first data transformation of a pair of complementary data transformations of source test data which produce resultant test data, said first data transformation being according to said first public/private key encryption algorithm using said identity public key;

(d) directs said digital protection system to perform a second data transformation of said pair of complementary data transformations of source test data which produce resultant test data, said second data transformation being complementary to said first data transformation;

(e) compares said source test data with said resultant test data; and

(f) verifies information concerning the tangible object responsive to steps (b) and (e).

45. (Original) The apparatus for verifying information concerning a tangible object of claim 44, wherein said digital protection system interface is a physical coupling which supplies power to said digital protection system.

46. (Original) The apparatus for verifying information concerning a tangible object of claim 44, wherein said digital protection system interface is a remote transmission interface.

47. (Original) The apparatus for verifying information concerning a tangible object of claim 44, wherein said digital signature represents an encryption of data derived from said identity public key and said attribute data according to a derivation algorithm, said encryption being according to a second public/private key encryption algorithm using a signature private key, and wherein said protection system verification program verifies that said digital signature matches said identity public key and said attribute data by:

decrypting said digital signature according to said second public/private key encryption algorithm using a signature public key;

deriving data from said identity public key and said attribute data using said derivation algorithm; and

comparing the decrypted digital signature to the data derived from said identity public key and said attribute data according to said derivation algorithm.

48. (Original) The apparatus for verifying information concerning a tangible object of claim 44, wherein said first data transformation is an encryption of said source test data and said second data transformation is a decryption of said source test data encrypted by said first data transformation, said first data transformation being performed before said second data transformation..

49. (Original) The apparatus for verifying information concerning a tangible object of claim 44, wherein said second data transformation is an encryption of said source test data and said first data transformation is a decryption of said source test data encrypted by said second data transformation, said second data transformation being performed before said first data transformation.

50. (Original) The apparatus for verifying information concerning a tangible object of claim 44, wherein said source test data is randomly generated data.

51-90. (Cancelled)

97. (Currently Amended) A personal identity document for a ~~subject~~ natural person, comprising:

a portable, tangible carrier for carrying by said natural person; and

a digital protection system physically attached to said carrier, said digital protection system comprising:

(a) an external interface for receiving data requests,

(b) a processor coupled to said external interface, said processor capable of performing a data transformation according to a first public/private key encryption algorithm, and

(c) an internal data storage, said internal data storage storing an identity private key and a data descriptor, said identity private key being inaccessible outside said external interface, said data descriptor including an identity public key, attribute data relating to attributes of said natural person, and a digital signature of said identity public key and said attribute data, said identity public key corresponding to said identity private key according to said first public/private key encryption algorithm;

wherein said processor performs said data transformation of data responsive to a request received through said external interface, said processor performing said data transformation according to said first public/private key encryption algorithm using said identity private key.

98. (Currently Amended) The personal identity document of claim 97, wherein said attribute data comprises data identifying a digitized photographic image of said ~~subject~~ natural person.

99. (Currently Amended) The personal identity document of claim 97, wherein said attribute data comprises data identifying said ~~subject~~ natural person according to at least one physical characteristic verified by a digital data processing device.

100. (Currently Amended) The personal identity document of claim 99, wherein said data identifying ~~a~~ said natural person according to at least one physical characteristic comprises data derived from an iris scan.

101. (Currently Amended) The personal identity document of claim 99, wherein said data identifying ~~a~~ said natural person according to at least one physical characteristic comprises data derived from an retina scan.

102. (Currently Amended) The personal identity document of claim 99, wherein said data identifying ~~a~~ said natural person according to at least one physical characteristic comprises data derived from a voice sample.

103. (Original) The personal identity document of claim 97, wherein said digital signature is an encryption of data derived from said identity public key and attribute data, said encryption being according to a second public private key encryption algorithm using a signature private key, said digital signature being capable of decoding according to said second public/private key encryption algorithm using a signature public key.

104. (Original) The personal identity document of claim 103, wherein said digital signature is an encryption of data derived from said identity public key and attribute data by performing a pre-defined hash function.

105. (Original) The apparatus of claim 97, wherein said digital protection system is implemented in digital logic contained on a single integrated circuit substrate.

106. (Currently Amended) A control station for verifying the respective personal identities of multiple ~~subjects~~ natural persons, comprising:

a programmable processor;

a memory, said memory storing a control program which executes on said programmable processor and controls at least some operations of said control station;

a digital personal identity document interface, said interface communicating with a digital personal identity document of a ~~subject~~ natural person, said digital personal identity document being a portable, tangible device carried by said natural person;

wherein said control program verifies a personal identity of a ~~subject~~ natural person by:

(a) obtaining a data descriptor from said digital personal identity document of the subject through said interface, said descriptor comprising an identity public key for transforming data according to a first public/private key encryption algorithm, attribute data containing identifying information concerning said ~~subject~~ natural person, and a digital signature;

(b) verifying that said digital signature matches said identity public key and said attribute data;

(c) performing a pair of complementary data transformations of source test data to produce resultant test data, said pair of complementary data transformations including (i) a first data transformation according to said first public/private key encryption algorithm using said identity public key, said first data transformation being performed externally to said digital personal identity document, and (ii) a second data transformation according to said first public/private key encryption algorithm, said second data transformation being performed by said digital personal identity document responsive to a request by said control program;

(d) comparing said source test data with said resultant test data; and

(e) verifying the identity of said ~~subject~~ natural person depending on the results of said step of verifying that said digital signature matches said identity public key and said attribute data, and said step of comparing said source test data with said resultant test data.

107. (Currently Amended) The control station for verifying the respective identities of multiple ~~subjects~~ natural persons of claim 106, wherein said control station is a passport control station at a jurisdictional entry or exit location.

108. (Currently Amended) The control station for verifying the respective identities of multiple ~~subjects~~ natural persons of claim 106, further comprising an operator interface displaying information to an operator, said information including a result of steps (b) and (d).

109. (Currently Amended) The control station for verifying the respective identities of multiple ~~subjects~~ natural persons of claim 108, wherein said information displayed to said operator further comprises at least some identifying information derived from said attribute data..

110. (Currently Amended) The control station for verifying the respective identities of multiple ~~subjects~~ natural persons of claim 109, wherein said identifying information derived from said attribute data comprises a digitized photographic image of said subject.

111. (Currently Amended) The control station for verifying the respective identities of multiple ~~subjects~~ natural persons of claim 106, further comprising a physical characteristic sensing device, said physical characteristic sensing device automatically sensing at least one physical characteristic of the subject, said at least one physical characteristic being compared to identifying data contained in said data descriptor to verify the identity of said subject.

112. (Currently Amended) The control station for verifying the respective identities of multiple ~~subjects~~ natural persons of claim 111, wherein said physical characteristic sensing device is an iris scanning device.

113. (Currently Amended) The control station for verifying the respective identities of multiple ~~subjects~~ natural persons of claim 106, wherein said digital signature represents an encryption of data derived from said identity public key and said attribute data according to a derivation algorithm, said encryption being according to a second public/private key encryption algorithm using a signature private key, and wherein said control program verifies that said digital signature matches said identity public key and said attribute data by:

decrypting said digital signature according to said second public/private key encryption algorithm using a signature public key;

deriving data from said identity public key and said attribute data using said derivation algorithm; and

comparing the decrypted digital signature to the data derived from said identity public key and said attribute data according to said derivation algorithm.

114. (Currently Amended) The control station for verifying the respective identities of multiple ~~subjects~~ natural persons of claim 106, wherein said first data transformation is an encryption of said source test data and said second data transformation is a decryption of said source test data encrypted by said first data transformation, said first data transformation being performed before said second data transformation.

115. (Currently Amended) The control station for verifying the respective identities of multiple ~~subjects~~ natural persons of claim 106, wherein said second data transformation is an encryption of said source test data and said first data transformation is a decryption of said source test data encrypted by said second data transformation, said second data transformation being performed before said first data transformation.

116. (Currently Amended) The control station for verifying the respective identities of multiple ~~subjects~~ natural persons of claim 106, wherein said source test data is randomly generated data.

117. (Currently Amended) A method for verifying the identity of a ~~subject~~ natural person, comprising the steps of:

(a) obtaining a data descriptor from a digital personal identity document of the ~~subject~~ natural person, said digital personal identity document being a portable, tangible device carried by said natural person, said descriptor comprising an identity public key for transforming data according to a first public/private key encryption algorithm, attribute data containing identifying information concerning said ~~subject~~ natural person, and a digital signature;

(b) verifying that said digital signature matches said identity public key and said attribute data;

(c) performing a pair of complementary data transformations of source test data to produce resultant test data, wherein a first data transformation of said pair is performed by a verifying device according to said first public/private key encryption algorithm using said identity public key, and wherein a second data transformation of said pair is performed by said digital personal identity document responsive to a request from a verifying device, said second data transformation being complementary to said first data transformation;

(d) comparing said source test data with said resultant test data; and

(e) verifying the identity of said ~~subject~~ natural person responsive to the results of steps (b) and (d).

118. (Currently Amended) The method for verifying the identity of a ~~subject~~ natural person of claim 117, wherein said digital signature represents an encryption of data derived from said identity public key and said attribute data ~~according~~, said encryption being according to a second public/private key encryption algorithm using a signature private key, and wherein step (b) comprises the steps of:

decrypting said digital signature according to said second public/private key encryption algorithm using a signature public key;

comparing the decrypted digital signature to said data derived from said identity public key and said attribute data.

119. (Currently Amended) The method for verifying the identity of a ~~subject~~ natural person of claim 118, wherein said digital signature is an encryption of data derived from said identity public key and attribute data by performing a pre-defined hash function.

120. (Currently Amended) The method for verifying the identity of a ~~subject~~ natural person of claim 117, wherein said first data transformation is an encryption of said source test data and said second data transformation is a decryption of said source test data encrypted by said first data transformation, said first data transformation being performed before said second data transformation..

121. (Currently Amended) The method for verifying the identity of a ~~subject~~ natural person of claim 117, wherein said second data transformation is an encryption of said source test data and said first data transformation is a decryption of said source test data encrypted by said second data transformation, said second data transformation being performed before said first data transformation.

122. (Currently Amended) The method for verifying the identity of a ~~subject~~ natural person of claim 117, further comprising the step of displaying information to an operator, said information including a result of step (e).

123. (Currently Amended) The method for verifying the identity of a ~~subject~~ natural person of claim 122, wherein said information displayed to said operator further comprises at least some identifying information derived from said attribute data..

124. (Currently Amended) The method for verifying the identity of a ~~subject~~ natural person of claim 123, wherein said identifying information derived from said attribute data comprises a digitized photographic image of said ~~subject~~ natural person.

125. (Currently Amended) The method for verifying the identity of a ~~subject~~ natural person of claim 117, further comprising the steps of:

automatically sensing at least one physical characteristic of the ~~subject~~ natural person with a sensing device; and

automatically comparing said at least one physical characteristic to identifying data contained in said data descriptor to verify the identity of said ~~subject~~ natural person.

126. (Currently Amended) The method for verifying the identity of a ~~subject~~ natural person of claim 125, wherein said sensing device is an iris scanning device.

127. (Currently Amended) The method for verifying the identity of a ~~subject~~ natural person of claim 117, wherein said source test data is randomly generated data.

128 - 140. (Cancelled)

141. (New) The method for updating attribute data of claim 28, wherein said identity public key, said old attribute data and said old digital signature are obtained from said digital protection mechanism, said method further comprising the step of storing said updated descriptor in said digital protection mechanism.

142. (New) The apparatus of claim 97, wherein said carrier contains at least some of said attribute data printed in human readable form.

143. (New) A method for using verified information concerning a tangible object, comprising the steps of:

accessing descriptor data associated with the tangible object, said tangible object being other than a data processing device, said descriptor data including an identity public key for transforming data according to a first public/private key encryption algorithm, attribute data containing information concerning said tangible object, and a digital signature;

verifying that said digital signature matches said identity public key and said attribute data;

performing a pair of complementary data transformations on source test data to produce resultant test data, said pair of complementary data transformations being performed by:

(a) performing a first data transformation according to said first public/private key encryption algorithm using said identity public key, and

(b) accessing a digital protection system physically attached to said tangible object to perform a second data transformation according to said first public/private key encryption algorithm using an identity private key in said digital protection system, said identity private key corresponding to said identity public key according to said first public/private key encryption algorithm, said second data transformation being complementary to said first data transformation;

comparing said source test data with said resultant test data; and

using said attribute data in a manner dependent on the results of said step of verifying that said digital signature matches said identity public key and said attribute data, and said step of comparing said source test data with said resultant test data.

144. (New) The method for using verified information concerning a tangible object of claim 143, wherein said digital signature represents an encryption of data derived from said identity public key and said attribute data according to a derivation algorithm, said encryption being according to a second public/private key encryption algorithm using a signature private key, and wherein said step of verifying that said digital signature matches said identity public key and said attribute data comprises:

decrypting said digital signature according to said second public/private key encryption algorithm using a signature public key;

deriving data from said identity public key and said attribute data using said derivation algorithm; and

comparing the decrypted digital signature to the data derived from said identity public key and said attribute data according to said derivation algorithm.

145. (New) The method for using verified information concerning a tangible object of claim 144, wherein said derivation algorithm comprises a hash function.

146. (New) The method for using verified information concerning a tangible object of claim 144, wherein said derivation algorithm is an identity function which produces as output an identical copy of the input.

147. (New) The method for using verified information concerning a tangible object of claim 143, wherein said first data transformation is an encryption of said source test data and said second data transformation is a decryption of said source test data encrypted by said first data transformation, said first data transformation being performed before said second data transformation.

148. (New) The method for using verified information concerning a tangible object of claim 143, wherein said second data transformation is an encryption of said source test data and said first data transformation is a decryption of said source test data encrypted by said second data transformation, said second data transformation being performed before said first data transformation.

149. (New) The method for using verified information concerning a tangible object of claim 143, wherein said step of accessing descriptor data comprises obtaining said descriptor data from said digital protection system.

150. (New) The method for using verified information concerning a tangible object of claim 143, wherein said source test data is randomly generated data.

151. (New) The method for using verified information concerning a tangible object of claim 143, wherein said digital protection system of said tangible object includes a coupling for mating with a local digital data processing device separate from said tangible object.